Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A monolithic semiconductor integrated circuit for selectively encrypting or decrypting data, comprising:

a plurality of devices each having a unique identifier;

a cryptographic circuit arranged to encrypt or decrypt data;

a plurality of selectable data routes formed from a plurality of data pathways, along which data may flow between the devices and an external memory, wherein at least one data route passes through the cryptographic circuit and at least one data route does not pass through the cryptographic circuit; and

a control arranged to receive the unique identifier of a selected one of the devices transferring data, and to select one of the at least one data route that passes through the cryptographic circuit, or one of the at least one data route that does not pass through the cryptographic circuit, according to the unique identifier of the selected device.

2. (Previously Presented) A semiconductor integrated circuit according to claim 1 wherein the control is further arranged to select a route that passes through the cryptographic circuit if the control determines that the device transferring data is secure.

3. (Previously Presented) A semiconductor integrated circuit according to claim 1 wherein the control is further arranged to select a route that does not pass through the cryptographic circuit if the control determines that the device transferring data is insecure.

4. (Previously Presented) A semiconductor integrated circuit according to claim 3 wherein the control is arranged to use the unique identifier to determine that the selected device is secure or insecure.

5. (Previously Presented) A semiconductor integrated circuit according to claim 4 wherein the control is further arranged to use the unique identifier as an index to a look-up table containing an indication of which of the devices are secure or insecure.

6. (Previously Presented) A semiconductor integrated circuit according to claim 1 wherein the plurality of devices includes at least one of, a cryptographic processor, direct memory access unit, central processing unit, moving picture experts group decoder, read only memory, programmable transport interface, universal serial bus interface, or broadcast receiver.

7. (Previously Presented) A semiconductor integrated circuit according to claim 1 wherein the data includes video data, audio data, encryption keys, or data broadcast over air.

8. (Previously Presented) A semiconductor integrated circuit according to claim 1, wherein the control is further arranged to cause the cryptographic circuit to encrypt data transmitted from a first device of the devices to the external memory only if the first device is secure, and to cause the cryptographic circuit to decrypt data from the external memory to a second device of the devices only if the second device is secure.

9. (Previously Presented) A semiconductor integrated circuit according to claim 1 wherein the external memory is separated into a plurality of mutually exclusive regions, and the circuit further comprises:

a register for storing data for distinguishing the regions of the external memory; and

a filter through which the data routes connecting the devices and the external memory pass, arranged to selectively block a data access to or from the external memory according to the unique identifier of a device, of the devices, requesting the data access, and according to which region of the external memory is being accessed.

10. (Previously Presented) A semiconductor integrated circuit according to claim 9 wherein some of the regions of the external memory store privileged data, and the other regions of the external memory store unprivileged data.

11. (Previously Presented) A semiconductor integrated circuit according to claim 9 wherein the register is arranged to store start and end memory addresses of each region of the external memory.

12. (Previously Presented) A semiconductor integrated circuit according to claim 11 wherein the filter is arranged to compare a memory address of data being accessed with contents of the register to determine which region of the external memory is being accessed.

13. (Original) A semiconductor integrated circuit according to claim 12 wherein the filter is arranged to selectively block data accesses requested by secure devices to unprivileged regions of data.

14. (Original) A semiconductor integrated circuit according to claim 12 wherein the filter is arranged to selectively block data accesses requested by insecure devices to privileged regions of data.

15. (Previously Presented) A semiconductor integrated circuit according to claim 1 wherein the semiconductor integrated circuit is a television decoder.

16. (Currently Amended) A method, comprising:

transmitting data between one of a plurality of devices, the devices each having a unique identifier, and an external memory, the data being transmitted along one of a plurality of selectable data routes formed from a plurality of data pathways, wherein at least one data route passes through a cryptographic circuit and at least one data route does not pass through the cryptographic circuit; and

selectively encrypting or decrypting the transmitted data, the selectively encrypting or decrypting including:

receiving the identification of a selected one of the devices; and

selecting a data route of the at least one data route that passes through the cryptographic circuit, or one of the at least one data route that does not pass through the cryptographic circuit, according to the unique identifier of the selected device.

17. (Original) The method according to claim 16 further comprising the steps of determining that the device transferring data is secure, and selecting a data route that passes through the cryptographic circuit if the device is secure.

18. (Original) The method according to claim 16 further comprising the steps of determining that the device transferring data is insecure, and selecting a data route that does not pass through the cryptographic circuit if the device is insecure.

19. (Previously Presented) The method according to claim 18 further comprising the step of using the unique identifier to determine whether the selected device is secure or insecure.

20. (Previously Presented) The method according to claim 19 further comprising the step of using the unique identifier as an index to a look-up table containing an indication of which of the devices are secure or insecure.

21. (Previously Presented) The method according to claim 16 wherein the plurality of devices includes at least one of, a crypto core, direct memory access unit, central processing unit, moving picture experts group decoder, read only memory, programmable transport interface, universal serial bus interface, or broadcast receiver.

22. (Previously Presented) The method according to claim 16 wherein the data includes video data, audio data, encryption keys, or data broadcast over air.

23. (Previously Presented) The method according to claim 16 further comprising the steps of:

transmitting data from a first device of the devices to the external memory;

encrypting the data only if the first device is secure;

transmitting the data from the external memory to a second device of the devices; and

decrypting the data only if the second device is secure.

24. (Previously Presented) The method according to claim 16 wherein the external memory is separated into a plurality of mutually exclusive regions, the method further comprising the steps of:

determining which region of the external memory is being accessed;

selectively blocking a data access to or from the external memory according to the unique identifier of a device, of the devices, requesting the data access, and according to which region of the external memory is being accessed.

25. (Original) The method according to claim 24 wherein some of the regions of the external memory store privileged data, and the other regions of the external memory store unprivileged data.

26. (Previously Presented) The method according to claim 24 wherein the step of determining which region of the external memory is being accessed comprises the step of comparing a memory address of the data being accessed with start and end memory addresses of each region of the external memory.

27. (Original) The method according to claim 26 wherein data accesses requested by secure devices to unprivileged regions of data are selectively blocked.

28. (Original) The method according to claim 26 wherein data accesses requested by insecure devices to privileged regions of data are selectively blocked.

29. (Currently Amended) A system, comprising:

an external memory; and

a monolithic semiconductor integrated circuit for selectively encrypting or decrypting data, the semiconductor integrated circuit including:

a plurality of devices each having a unique ~~identifier~~ identifier;

a cryptographic circuit arranged to encrypt or decrypt data;

a plurality of selectable data routes formed from a plurality of data pathways, along which data may flow between the devices and the external memory, wherein at least one data route passes through the cryptographic circuit and at least one data route does not pass through the cryptographic circuit; and

a control arranged to receive the unique identifier of a selected one of the devices transferring data, and to select one of the at least one data route that passes through the cryptographic circuit, or one of the at least one data route that does not pass through the cryptographic circuit, according to the unique identifier of the selected device.

30. (Previously Presented) A system according to claim 29 wherein the control is further arranged to select a route that passes through the cryptographic circuit if the control determines that the device transferring data is secure.

31. (Previously Presented) A system according to claim 29 wherein the control is further arranged to select a route that does not pass through the cryptographic circuit if the control determines that the device transferring data is insecure.

32. (Previously Presented) A system according to claim 29 wherein the control is further arranged to use the unique identifier as an index to a look-up table containing an indication of which of the devices are secure or insecure.

33. (Previously Presented) A system according to claim 29, wherein the control is further arranged to cause the cryptographic circuit to decrypt data from the external memory to one of the devices only if the one of the devices is secure.

34. (Previously Presented) A system according to claim 29 wherein the external memory is separated into a plurality of mutually exclusive regions, and the circuit further comprises:

a register for storing data for distinguishing the regions of the external memory; and

a filter through which the data routes connecting the devices and the external memory pass, arranged to selectively block a data access to or from the external memory according to the unique identifier of a device, of the devices, requesting the data access, and according to which region of the external memory is being accessed.

35. (Previously Presented) A system according to claim 34 wherein the filter is arranged to selectively block data accesses requested by secure devices to unprivileged regions of data.

36. (Previously Presented) A system according to claim 34 wherein the filter is arranged to selectively block data accesses requested by insecure devices to privileged regions of data.